ZARZĄDZENIE Nr 9/2017
Dyrektora Centrum Usług Wspólnych w Gminie Żabia Wola
w Gminie Żabia Wola

z dnia 4 kwietnia 2017 r.

w sprawie wprowadzenia w Centrum Usług Wspólnych w Gminie Żabia Wola Polityki bezpieczeństwa i ochrony przetwarzania danych osobowych.

Na podstawie: art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. 2016 r. poz. 922) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) zarządza się, co następuje:

§ 1.

1. Wprowadza się do stosowania w Centrum Usług Wspólnych w Gminie Żabia Wola Politykę bezpieczeństwa i ochrony przetwarzania danych osobowych, w brzmieniu stanowiącym ***Załącznik*** do niniejszego zarządzenia.
2. Do stosowania zasad określonych w Polityce bezpieczeństwa zobowiązani są wszyscy pracownicy Centrum Usług Wspólnych w Gminie Żabia Wola oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 2.

Zarządzenie wchodzi w życie w dniem podpisania.

DYREKTOR
Justyna Wodnicka-Żuk

ZAŁĄCZNIK do Zarządzenia Nr 9/2017
Dyrektora Centrum Usług Wspólnych
w Gminie Żabia Wola z dnia 4 kwietnia 2017 r.
w sprawie wprowadzenia Polityki bezpieczeństwa
i ochrony przetwarzania danych osobowych w Centrum
Usług Wspólnych w Gminie Żabia Wola

POLITYKA BEZPIECZEŃSTWA I OCHRONY PRZETWARZANIA DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA

§ 1.
POSTANOWIENIA OGÓLNE, DEFINICJE

1. Polityka bezpieczeństwa i ochrony przetwarzania danych osobowych jest zbiorem zasad i procedur obowiązujących w Centrum Usług Wspólnych w Gminie Żabia Wola przy przetwarzaniu danych osobowych w formie tradycyjnej jak i za pośrednictwem systemów informatycznych.
2. Celem Polityki bezpieczeństwa i ochrony przetwarzania danych osobowych jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania danych osobowych, a przede wszystkim zapewnienie ochrony tych danych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.
3. Dokumentacja została opracowana na podstawie:
   1) art. 47 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (t. j. Dz. U. z 1997 r. Nr 78 poz. 483);
   2) Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (*t. j. Dz. U. 2016 r. poz. 922*);
   3) Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz. U. z 2004 r. nr 100, poz. 1024*);
   4) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne *(t. j. Dz. U. z 2014 r. poz. 1114 z późn. zm.);*
   5) Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych *(t. j. Dz. U. z 2016 r. poz. 113).*

§ 2.

Ilekroć w niniejszej Polityce jest mowa o::

1) **„UODO, Ustawie”** – należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2016 poz. 922);
2) **„Polityce bezpieczeństwa”**- należy przez to rozumieć niniejszą Politykę bezpieczeństwa i ochrony przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola;
3) **„Centrum, Jednostce”** – należy przez to rozumieć Centrum Usług Wspólnych w Gminie Żabia Wola;

4) **„Administratorze Danych Osobowych”**- należy przez to rozumieć Centrum Usług Wspólnych w Gminie Żabia Wola reprezentowane przez Dyrektora, zwane dalej „ADO”;
5) **„osobie upoważnionej lub użytkowniku systemu”**- należy przez to rozumieć osobę posiadającą upoważnienie wydane przez ADO i dopuszczoną do przetwarzania danych osobowych w systemie informatycznym w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem”;
6) **„osobach zatrudnionych przy przetwarzaniu danych osobowych”** – należy przez to rozumieć wszystkie osoby, w tym użytkowników systemu informatycznego, mające dostęp do danych osobowych;
7) **„zbiorze danych osobowych”** – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
8) **„systemie informatycznym”** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
9) **„stacji roboczej”** – należy przez to rozumieć stacjonarny lub przenośny komputer wchodzący w skład systemu informatycznego umożliwiający użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;
10) **„przetwarzaniu danych osobowych”** – należy przez to rozumieć wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie;
11) **„zbieraniu danych (gromadzeniu)”**- należy przez to rozumieć czynność początkową czyli wejście w posiadanie danych osobowych w dowolny sposób;
12) **„usuwaniu danych (niszczeniu)”**- należy przez to rozumieć czynność końcową czyli fizyczne niszczenie danych lub taką ich modyfikację, która uniemożliwia ustalenie osoby, której dane dotyczą;
13) **„utrwalaniu”**- należy przez to rozumieć zapisanie informacji (danych osobowych) na materialnym nośniku (papier, dysk twardy);
14) **„zmienianiu”**- należy przez to rozumieć działanie polegające na weryfikacji i aktualizacji posiadanych danych osobowych;
15) **„udostępnianiu danych osobowych”**- należy przez to rozumieć objęcie w posiadanie danych osobowych przez innego administratora danych osobowych;
16) **„opracowywaniu danych osobowych”**- należy przez to rozumieć wykorzystanie danych osobowych zawartych w zbiorze w celu uzyskania zamierzonego rezultatu;
17) **„przechowywaniu danych osobowych”**- należy przez to rozumieć posiadanie danych osobowych;
18) **„anonimizacji dokumentu”** – należy przez to rozumieć czynność polegającą na wykreśleniu z treści dokumentu różnych elementów, aby uniemożliwić identyfikację występujących w nim danych osobowych;
19) **poufności danych** – należy przez to rozumieć właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

20) **integralności danych** – należy przez to rozumieć właściwość zapewniająca, że dane osobowe nie zostały zmienione, lub zniszczone w sposób nieautoryzowany;
21) **rozliczalność** – należy przez to rozumieć właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

§ 3.
ZARZĄDZANIE PRZETWARZANIEM DANYCH OSOBOWYCH

1. Za przetwarzanie danych osobowych oraz ich ochronę w Centrum odpowiadają:
   1) Administrator Danych Osobowych;
   2) każda osoba wykonująca pracę bądź świadcząca usługi cywilnoprawne na rzecz Administratora Danych Osobowych, która uzyskała upoważnienie do przetwarzania danych osobowych.
2. Administrator Danych Osobowych (ADO):
   1) decyduje o celach i środkach przetwarzania danych osobowych;
   2) odpowiada za organizację bezpieczeństwa i ochrony przetwarzania danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych;
   3) zapewnia przetwarzania danych zgodnie z uregulowaniami niniejszej Polityki bezpieczeństwa;
   4) wydaje i anuluje upoważnienia do przetwarzania danych osobowych;
   5) dokonuje natychmiastowych zmian uprawnień określonych w upoważnieniu pracownika w związku ze zmianą zakresu jego obowiązków;
   6) prowadzi nadzór nad prawidłowością zapisów w umowach serwisowych podpisywanych z podmiotami zewnętrznymi, tak aby gwarantowały one odpowiedni poziom bezpieczeństwa danych.
   7) podpisuje i nadzoruje zapisy w umowach powierzenia przetwarzania danych zawieranych z innymi podmiotami;
   8) zapewnia przestrzeganie przepisów o ochronie danych osobowych, w szczególności przez:
      a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
      b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2 Ustawy, oraz przestrzegania zasad w niej określonych,
      c) zapoznanie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych (w formie szkoleń).
   9) zgłasza zbiory do GIODO i je aktualizuje jeśli jest taka potrzeba;
   10) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych;
   11) prowadzi ewidencję osób zapoznanych z Polityką bezpieczeństwa i przepisami ochronie danych osobowych;
   12) prowadzi i aktualizuje wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
   13) inicjuje i przeprowadza szkolenia pracowników w zakresie ochrony danych osobowych;
   14) nadzoruje naprawy, konserwacje oraz likwidacje urządzeń, na których zapisane są dane osobowe;
   15) nadzoruje obieg oraz przechowywanie dokumentów zawierających dane osobowe;
   16) nadzoruje prawidłowość archiwizacji oraz procesu usuwania danych osobowych;
   17) wdraża nowe rozwiązania w zakresie zabezpieczeń;
   18) prowadzi postępowania wyjaśniające w przypadku naruszenia ochrony danych osobowych;

19) kontroluje wykonywanie obowiązków służbowych pracowników pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
20) nadaje uprawnienia do przetwarzania danych osobowych w systemach informatycznych;
21) nadzoruje stosowanie środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;
22) sprawuje nadzór nad przechowywanymi kopiami zapasowymi opisanymi w instrukcji zarządzania systemem informatycznym.

3. Administrator Danych Osobowych realizując Politykę bezpieczeństwa dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem;
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane przetwarzaniu niezgodnemu z tymi celami;
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.
4. Administrator Danych Osobowych dąży do systematycznego unowocześniania stosowanych na terenie Jednostki informatycznych, technicznych i organizacyjnych środków ochrony tych danych w celu zabezpieczenia danych osobowych przed ich udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

§ 4.

7. W celu realizacji swoich obowiązków, ADO ma prawo:
   1) kontrolować stanowiska pracy Centrum w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
   2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą;
   3) wydawać polecenia pracownikom w zakresie bezpieczeństwa danych osobowych;
   4) żądać od wszystkich pracowników Jednostki wyjaśnień (ustnych lub pisemnych) w sytuacjach naruszenia bezpieczeństwa danych osobowych;
   5) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z zakresem kontroli;
   6) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

§ 5.

1. Każdy pracownik, który uzyskał upoważnienie do przetwarzania danych osobowych, zobowiązany jest do ich ochrony w sposób zgodny z przepisami Ustawy, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym.
2. Dostęp do określonego zbioru danych osobowych pracownik uzyskuje na podstawie pisemnego upoważnienia, otrzymanego w trybie określonym w niniejszej Polityce Bezpieczeństwa.
3. Pracownicy zatrudnieni – na podstawie umowy o pracę, bądź świadczący usługi na podstawie umów cywilnoprawnych – przy przetwarzaniu danych osobowych zobowiązani są do

zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

4. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych.
5. Osoby zatrudnione przy przetwarzaniu danych osobowych są w szczególności zobowiązani do:
   1) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji określonych w Polityce bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym;
   2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
   3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w niniejszej Polityce;
   4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
   5) nieudzielania informacji o danych osobowych przetwarzanych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
   6) bezzwłocznego zawiadamiania w formie pisemnej bądź ustnej Administratora Danych Osobowych o wszelkich nieprawidłowościach, przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe;
   7) zgłaszanie do ADO zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania zbiorów;
   8) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą.

§ 6.
OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH ORAZ ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w formie tradycyjnej oraz w systemach informatycznych w Jednostce odbywa się na obszarze wyznaczonym przez Administratora Danych Osobowych.
2. Obszar przetwarzania danych osobowych w obejmuje budynek Centrum, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje), oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
3. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz wykaz środków technicznych zastosowanych w celu ochrony danych osobowych stanowi ***Załącznik Nr 1*** do Polityki bezpieczeństwa;
4. Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko osoby upoważnione.

5. Przebywanie osób upoważnionych po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych Osobowych.
6. ADO może zezwolić na przebywanie w pomieszczeniach, o których mowa w ust. 3 niniejszego paragrafu, osobom sprzątającym te pomieszczenia poza godzinami pracy Centrum bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby zatrudnione na stanowiskach obsługi również podpisują klauzulę poufności, która zobowiązuje ich do zachowania w tajemnicy wszelkich informacji dotyczących Jednostki (*wzór określony jest w* ***Załączniku Nr 2*** *do Polityki bezpieczeństwa).*
7. W przypadku znalezienia dokumentacji zawierającej dane osobowe przez pracowników, o których mowa w ust 6 niniejszego paragrafu zobowiązani są oni do niezwłocznego odłożenia dokumentu do wydzielonej, do tego celu szafki, i poinformowania o zaistniałym fakcie Administratora Danych Osobowych.

8. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych.
9. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach, o których mowa w ust. 3 niniejszego paragrafu, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Administratora Danych Osobowych.
10. Dostęp osób trzecich do pomieszczeń, w których przetwarzane są dane osobowe jest możliwy podczas wykonywanych prac remontowych lub budowlanych wyłącznie pod nadzorem upoważnionego pracownika. Jeżeli jednak przebywanie w pomieszczeniu stwarza zagrożenie zdrowia lub życia pracownika, osoby trzecie mogą samodzielnie przebywać w tych pomieszczeniach. W tym przypadku akta, dokumenty oraz urządzenia i nośniki komputerowe zawierające dane osobowe powinny zostać przeniesione do innego pomieszczenia, bądź zabezpieczone w sposób zapewniający brak dostępu do nich osób trzecich.

§ 7.

1. ADO zobowiązany jest przeprowadzać przynajmniej raz na 6 m- cy bezpośrednią kontrolę stanu zabezpieczeń technicznych zbiorów danych osobowych.
2. Budynek i pomieszczenia, w których przetwarzane są dane osobowe, są zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
3. Każdy z pracowników Centrum posiada na stałe komplet kluczy, których posiadanie jest potwierdzone pisemnie w formie protokołu, którego wzór stanowi ***Załącznik Nr 3*** do niniejszej Polityki.
4. Dane osobowe przechowywane w wersji tradycyjnej (papierowej) lub elektronicznej (pamięć flash, płyty CD, DVD, dyskietki) po zakończeniu pracy są przechowywane w zamykanych na klucz meblach biurowych, a tam, gdzie jest to możliwe w szafach pancernych lub metalowych. (Wykaz zbiorów danych przetwarzanych w Centrum określony został w ***Załączniku Nr 4*** do Polityki bezpieczeństwa.)**.**
5. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich

modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

6. Sposób zniszczenia danych osobowych zależy do rodzaju nośnika danych oraz ich kategorii.

§ 8.

1. Do zabezpieczeń organizacyjnych należy:
   1) sporządzenie i wdrożenie Polityki bezpieczeństwa;
   2) sporządzenie i wdrożenie Instrukcji zarządzania systemem informatycznym;
   3) przeszkolenie pracowników w zakresie ochrony danych osobowych przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej.
   4) dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienia nadane przez Administratora Danych Osobowych. Wzór upoważnienia określa ***Załącznik Nr 5*** do Polityki Bezpieczeństwa;
   5) zachowanie zasady, przy nadawaniu upoważnień, że dostęp do danych będą miały tylko te osoby, którym jest to niezbędne do realizacji powierzonych im zadań i tylko w takim zakresie jaki jest konieczny do ich realizacji.
   6) prowadzenie przez ADO ewidencji osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi ***Załącznik Nr* 6** do Polityki bezpieczeństwa.
   7) stworzenie procedury postępowania w sytuacji naruszenia ochrony danych osobowych;
   8) zapoznanie (przeszkolenie) osób zatrudnionych przy przetwarzaniu danych z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   9) zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy;
   10) wprowadzenie procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych, określonej w obowiązującej Instrukcji zarządzania systemem informatycznym.
2. Za przeprowadzenie szkolenia, o którym mowa w ust. 1 pkt 4 niniejszego paragrafu odpowiada Administrator Danych Osobowych.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych i wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i Instrukcją zarządzania systemem informatycznym obowiązującą w Centrum.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza:
   1) listy uczestników szkolenia, która stanowi ***Załącznik Nr 7*** do Polityki Bezpieczeństwa;
   2) oświadczenia o zapoznaniu się z Polityką bezpieczeństwa i przepisami dotyczącymi ochrony danych osobowych oraz zobowiązaniu się do przestrzegania określonych w nich zasad przetwarzania i ochrony danych osobowych (wzór oświadczenia stanowi ***Załącznik Nr 8*** do Polityki bezpieczeństwa, a ewidencja osób zapoznanych z Polityką bezpieczeństwa i przepisami o ochronie danych osobowych, którą prowadzi Administrator Danych Osobowych stanowi ***Załącznik Nr 9*** do Polityki bezpieczeństwa). Podpisane oświadczenia przechowywane są w aktach osobowych pracowników.

§ 9.
PRZETWARZANIE DANYCH POZA OBSZAREM WYZNACZONYM PRZEZ ADMINISTRATORA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza obszarem przetwarzania danych wyłącznie za zgodą Administratora Danych Osobowych.
2. W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem wyznaczonym przez ADO, należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.
3. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowani poza obszarem przetwarzania danych osobowych, w tym stosuje hasła dostępu do komputera przenośnego, w którym przetwarzane są dane osobowe.
4. Po każdorazowym użyciu urządzenia przenośnego poza obszarem przetwarzania danych na koniec dnia tworzy się kopię zapasową.
5. Dokumenty w formie papierowej powinny być odpowiednio zabezpieczone (np. w teczkach) i w żadnym wypadku nie mogą mieć do nich dostępu osoby postronne.
6. Po zakończonej pracy poza obszarem wyznaczonym przez ADO należy niezwłocznie zwrócić dokumenty do Jednostki, a jeśli jest to niemożliwe należy je przechowywać w domu, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych.
7. Fakt zabrania ze sobą przez pracownika dokumentów lub sprzętu przenośnego, celem przetwarzania danych tam zawartych poza obszarem wyznaczonym przez Administratora Danych Osobowych, jest każdorazowo odnotowywany w prowadzonej ewidencji pobrania/ zdania sprzętu czy dokumentów. (Wzór ewidencji stanowi ***Załącznik Nr 10*** do niniejszej Polityki bezpieczeństwa).

§ 10.
PRZETWARZANIE DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych jest możliwe wyłącznie gdy:
   1) jest to niezbędne do realizacji uprawnień, lub spełnienia obowiązków wynikających z przepisów prawa;
   2) jest to niezbędne do zrealizowania umowy, gdy osoba, której dane dotyczą jest jej stroną lub jest to konieczne do podjęcia działań przed zawarciem umowy;
   3) jest konieczne do wykonania określonych prawnie zadań realizowanych dla dobra publicznego;
   4) jest to konieczne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez jednostkę, a przetwarzanie nie narusza praw i wolności osób, której dane dotyczą;
   5) osoba, której dane dotyczą, wyrazi pisemną zgodę na przetwarzanie danych osobowych. Zgoda nie może być domniemana lub dorozumiana. Zgoda musi być dobrowolna i zawarta z zachowaniem równowagi pomiędzy dającym zgodę, a Administratorem Danych Osobowych.
2. W przypadku legalności przetwarzania danych wynikających z ust. 1 pkt 1 - 4 niniejszego paragrafu Jednostka nie musi występować o zgodę na przetwarzanie danych osobowych.
3. Przetwarzanie danych wrażliwych możliwe jest wyłącznie gdy:
   1) osoba, której dane dotyczą wyrazi na to pisemną zgodę;
   2) przepis szczególny innej ustawy niż UODO zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;

3) przetwarzanie takich danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą.

§ 11.
OBOWIĄZEK INFORMACYJNY

1. Dane osobowe przetwarzane w Centrum mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą, lub z innych źródeł, w granicach dozwolonych przepisami prawa.
2. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
3. W przypadku gdy dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem UODO albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.
4. W przypadku gdy dane pochodzą bezpośrednio od osób, których dotyczą, pracownicy Jednostki są odpowiedzialni za poinformowanie tych osób, o:
   1) adresie siedziby Centrum, pod którym dane są zbierane i przetwarzane;
   2) celu zbierania danych;
   3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
   4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
5. Obowiązek informacyjny wypełniany jest przed pozyskaniem danych.
6. Wzór informacji określa ***Załącznik Nr 11*** do Polityki bezpieczeństwa.
7. Podpisane zapoznanie się z informacją przez osobę, której dane dotyczą jest potwierdzeniem spełnienia obowiązku informacyjnego przez ADO.

§ 12.
UDOSTĘPNIANIE DANYCH OSOBOWYCH

1. Administrator Danych Osobowych udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
   3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi ***Załącznik Nr 12*** do Polityki Bezpieczeństwa.
4. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

6. Administrator Danych Osobowych zachowuje szczególną staranność i nadzór w zakresie udostępniania danych osobowych.
7. Udostępnienie danych nie może naruszać praw i wolności osób, których one dotyczą;
8. W celu nadzoru nad udostępnianiem danych osobowych prowadzona jest ewidencja udostępniania danych osobowych, której wzór stanowi ***Załączniku Nr 13*** do Polityki bezpieczeństwa.
9. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 13.

1. Każda osoba, której dane są przetwarzane w zbiorach Centrum ma prawo złożyć pisemny wniosek celem:
   1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia Administratora Danych, adresu jego siedziby i pełnej nazwy;
   2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
   3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych;
   4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że Administrator Danych jest zobowiązany do zachowania, w tym zakresie, w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
   5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
   6) uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, o którym mowa w art. 26a ust. 2 UODO;
2. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania. (Wzór informacji stanowi ***Załącznik Nr 14*** do Polityki bezpieczeństwa).
3. Informacje, o których mowa w ust. 1 niniejszego paragrafu może otrzymać osoba zainteresowana nie częściej niż raz na 6 miesięcy.
4. Administrator Danych może odmówić osobie, której dane dotyczą udzielenia informacji, o których mowa w ust. 1 niniejszego paragrafu jeżeli spowodowałoby to:
   1) ujawnienie wiadomości zawierających informacje niejawne;
   2) istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób lub jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 14.

Wniosek o udostępnienie informacji składany jest bezpośrednio do Administratora Danych Osobowych, który podejmuje decyzję o udostępnieniu oraz przygotowuje dane osobowe do udostępnienia w zakresie wskazanym we wniosku.

§ 15.
POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 31 UODO na podstawie umowy zawartej na piśmie pomiędzy ADO, a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje ADO i tworzy stosowną umowę powierzenia przetwarzania danych osobowych innemu podmiotowi.
3. Umowa, o której mowa w ust. 2 niniejszego paragrafu wyznacza zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych- wzór umowy powierzenia przetwarzania danych osobowych stanowi ***Załącznik Nr 15*** do Polityki bezpieczeństwa.
4. Każda osoba delegowana do wykonywania zadań na rzecz Jednostki, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
5. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
7. Podmiot, o którym mowa w ust. 1 niniejszego paragrafu, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie i celu określonym w umowie.
8. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.
9. Odpowiedzialność za przestrzeganie przepisów UODO spoczywa na Administratorze Danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

§ 16.
SPRAWDZENIA ZGODNOŚCI PRZETWARZANIA DANYCH Z PRZEPISAMI PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1. Dla zapewnienia prawidłowego przetwarzania danych i sprawdzenia skuteczności zastosowanych zabezpieczeń Administrator Danych Osobowych dokonuje okresowych sprawdzeń i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
2. Plan sprawdzeń przygotowywany jest przez ADO na okres nie krótszy niż kwartał i nie dłuższy niż rok.

3. Administrator Danych Osobowych w planie sprawdzeń uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych:
   1) z zasadami, o których mowa w art. 23- 37 i art. 31- 35 Ustawy;
   2) z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37- 39 Ustawy, w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
   3) z zasadami przekazywania danych osobowych, o których mowa w art. 47- 48 ustawy;

4) z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

4. Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem raz na pięć lat.
5. Sprawdzenie przeprowadzane jest w trybie:
   1) *sprawdzenia planowego* - według planu sprawdzeń określającego przedmiot, zakres oraz termin przeprowadzania poszczególnych sprawdzeń oraz sposób i zakres ich dokumentowania (wzór planu sprawdzeń określa ***Załącznik Nr 16*** do Polityki bezpieczeństwa);
   2) *sprawdzenia doraźnego* - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia przez Administratora Danych Osobowych wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia (wzór zgłoszenia podejrzenia naruszenia ochrony danych osobowych określa ***Załącznik Nr 17*** do Polityki bezpieczeństwa).
6. Ze sprawdzeń, o których mowa w ust. 5 niniejszego paragrafu, sporządza się sprawozdanie (w postaci papierowej bądź elektronicznej), które przechowuje Administrator Danych Osobowych (wzór sprawozdania określa ***Załącznik Nr 18*** do Polityki bezpieczeństwa). Sprawozdania tworzy się na potwierdzenie dokonania przez ADO czynności związanych ze sprawdzeniem.
7. Sprawdzenia są ewidencjonowane, a rejestr sprawdzeń stanowi ***Załącznik Nr 19*** do Polityki bezpieczeństwa.

§ 17.
POSTĘPOWANIE W PRZYPADKACH NARUSZENIA LUB PODEJRZENIA NARUSZENIA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Zasady postępowania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.
2. Naruszeniem bezpieczeństwa ochrony danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu osobom nieupoważnionym do danych osobowych lub pomieszczeń, w których się znajdują, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
   1) nieautoryzowany dostęp do danych;
   2) nieautoryzowane modyfikacje lub zniszczenie danych;
   3) udostępnienie danych nieautoryzowanym podmiotom;
   4) nielegalne ujawnienie danych;
   5) pozyskiwanie danych z nielegalnych źródeł;
   6) zmianę lub utratę danych zapisanych na kopiach zapasowych;
   7) naruszenie lub próby naruszenia poufności danych lub ich części;
   8) inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.
3. Przed przystąpieniem do pracy osoba upoważniona zobowiązana jest dokonać sprawdzenia stanu urządzeń komputerowych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

4. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany:
   1) przerwać przetwarzanie danych osobowych;
   2) zabezpieczyć elementy systemu informatycznego, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
   3) podjąć niezbędne działania w celu zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych;
   4) niezwłocznie powiadomić o tym fakcie ADO lub ewentualnie osobę przez niego upoważnioną (każdy z pracowników posiada nr telefonu do ADO).

5. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.
6. W sytuacjach, o których mowa w ust. 2 niniejszego paragrafu, ADO podejmuje działania mające na celu:
   1) minimalizację negatywnych skutków zdarzenia;
   2) wyjaśnienie okoliczności zdarzenia;
   3) zabezpieczenie dowodów zdarzenia,
   4) umożliwienie dalszego bezpiecznego przetwarzania danych.
7. Dla realizacji celów określonych w ust. 6 ADO ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
   1) żądania wyjaśnień od pracowników;
   2) korzystania z pomocy konsultantów;
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
8. Odmowa udzielenia wyjaśnień lub współpracy z ADO traktowana będzie jako naruszenie obowiązków pracowniczych.
9. ADO po opanowaniu sytuacji nadzwyczajnej opracowuje sprawozdanie, w którym przedstawia datę i godzinę powiadomienia, godzinę przybycia na miejsce zdarzenia, opis sytuacji zastanej, przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór sprawozdania z przebiegu zdarzenia stanowi ***Załącznik Nr 18*** do Polityki bezpieczeństwa- CZĘŚĆ 2. Sprawozdanie jest swego rodzaju potwierdzeniem dokonania danych czynności po otrzymaniu informacji o naruszeniu lub podejrzeniu naruszenia ochrony danych osobowych.
10. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Administratora Danych Osobowych.
11. W przypadku zaginięcia komputera lub nośników, na których były zgromadzone dane osobowe, użytkownik systemu niezwłocznie powiadamia Administratora Danych Osobowych, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

12. W sytuacji, o której mowa w ust. 11 niniejszego paragrafu Administrator Danych Osobowych podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zajęcia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.
13. W przypadku kradzieży komputera razem z nośnikiem ADO podejmuje działania zmierzające do odzyskania utraconych danych oraz monitoruje proces przebiegu wyjaśnienia sprawy.

§ 18.
POSTANOWIENIA KOŃCOWE

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych oraz do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień w nich zawartych.
2. Za przetwarzanie danych osobowych niezgodne z prawem, celami przetwarzania lub przechowywanie ich w sposób niezapewniający ochrony interesów osób, których te dane dotyczą grozi odpowiedzialność karna wynikająca z przepisów ustawy o ochronie danych osobowych lub pracownicza na zasadach określonych w Kodeksie pracy.

DYREKTOR
Justyna Wodnicka-Żuk

ZAŁĄCZNIK NR 1
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych
w Gminie Żabia Wola

OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE ORAZ ŚRODKI TECHNICZNE ZASTOSOWANE W CELU ZAPEWNIENIA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

Budynek i pomieszczenia	Zabezpieczenia budynku/ pomieszczenia	Zabezpieczenia zbiorów	Ilość stacji roboczych w pomieszczeniu	Zabezpieczenia komputerów
Budynek	Drzwi (metalowe) zamykane na klucz; okna (drewniane); alarm; monitoring; ochrona przeciwpożarowa- gaśnice,	…….	…….	…….
Pomieszczenie 1	(piętro); drzwi (zwykłe/ drewniane) zamykane na klucz; okna (drewniane); monitoring;	Szafy/ szafki/ biurko z szufladą/ szafa, szafka metalowa zamykane na klucz	1	Wewnętrzna sieć komputerowa zabezpieczona zaporą sieciową FireWall; indywidualna ochrona antywirusowa; każdy komputer wyposażony w hasło i login; monitory ustawione w sposób uniemożliwiający wgląd w dane osobowe osób wchodzących do pomieszczenia; wygaszacz ekranu, z którego wybudzenie wymaga wprowadzenia hasła użytkownika
Pomieszczenie 2	piętro; drzwi (zwykłe/drewniane) zamykane na klucz;	Szafy/ szafki/ biurko z szufladą/ szafa, zamykane na klucz	2	Wewnętrzna sieć komputerowa zabezpieczona zaporą sieciową FireWall; indywidualna ochrona antywirusowa; każdy komputer wyposażony w hasło i login; monitory ustawione w sposób uniemożliwiający wgląd w dane osobowe osób

				wchodzących do pomieszczenia; wygaszacz ekranu, z którego wybudzenie wymaga wprowadzenia hasła użytkownika
Pomieszczenie 3 serwerownia	piętro; drzwi (zwykłe/drewniane) zamykane na klucz;	Szafy/ szafki/ biurko z szufladą/ szafa, zamykane na klucz	2	Wewnętrzna sieć komputerowa zabezpieczona zaporą sieciową FireWall; indywidualna ochrona antywirusowa; każdy komputer wyposażony w hasło i login; monitory ustawione w sposób uniemożliwiający wgląd w dane osobowe osób wchodzących do pomieszczenia; wygaszacz ekranu, z którego wybudzenie wymaga wprowadzenia hasła użytkownika
Składnica akt	piętro/ ; drzwi (wzmocnione/ metalowe) zamykane na klucz; okna (drewniane); rolety antywłamaniowe w oknach; monitoring; alarm; ochrona przeciwpożarowa- gaśnica,	Regały;		

ZAŁĄCZNIK NR 2
do Polityki Bezpieczeństwa i
Ochrony Przetwarzania Danych
Osobowych w Centrum Usług
Wspólnych w Gminie Żabia Wola

……..…….. ……., dnia……...
(imię i nazwisko pracownika)

KLAUZULA POUFNOŚCI DANYCH

1. Zobowiązuję się do zachowania w tajemnicy służbowej tj. w szczególności do nie rozpowszechniania (bez zgody pracodawcy), w jakiejkolwiek formie, jakichkolwiek znanych mi informacji, wiadomości i materiałów dotyczących Centrum Usług Wspólnych w Gminie Żabia Wola, ul. Mazowiecka 1, 96- 321 Żabia Wola, do których będę miał(a) dostęp w związku z wykonywaniem obowiązków służbowych.
2. Zobowiązanie to obowiązuje przez okres trwania stosunku pracy oraz po jego ustaniu
3. Informacje, wiadomości i materiały objęte tajemnicą, o której mowa powyżej, to w szczególności: informacje o klientach i dostawcach, dane osobowe, dokumenty wytwarzane w toku pracy, korespondencja tradycyjna i elektroniczna, dane zawarte w pamięci komputerów i elektronicznych nośników informacji, należących do pracodawcy.

…….
(podpis pracownika)

ZAŁĄCZNIK NR 3
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych w
Gminie Żabia Wola

. . . . . , dn. . . . . .r.

PROTOKÓŁ
PRZEKAZANIA/ ZDANIA KLUCZY

Ja …… legitymujący się dowodem osobistym…….
(imię i nazwisko) (seria i numer)

Przejmuję/ zdaję* w dniu dzisiejszym, tj. ……., na wyłączne użytkowanie do celów służbowych komplet kluczy wejściowych do ……./ komplet kluczy do…… w związku z ustaniem stosunku pracy.*

Niniejszym zobowiązuję się do nieudostępniania ww. kluczy osobom trzecim. (wykreślić w przypadku potwierdzenia zdania kluczy)

…… ……
Przekazujący Przyjmujący

. . . . . , dn. . . . . .r.

…… ……
Przekazujący Przyjmujący

ZAŁĄCZNIK NR 4
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola

WYKAZ ZBIORÓW DANYCH PRZETWARZANYCH TRADYCYJNIE I W SYSTEMIE INFORMATYCZNYM

L.p.	Nazwa zbioru danych	Lokalizacja zbioru danych osobowych	Opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze	Autor i nazwa programu zastosowanego do przetwarzania danych	Opis przepływu pomiędzy systemami informatycznymi
1.	Dokumentacja wypadków pracowników	Pomieszczenie nr 1, 3	imię/nazwisko/imiona rodziców/data urodzenia/miejsce urodzenia/adres zamieszkania/PESEL/NIP/seria i nr dowodu osobistego/stan zdrowia	Microsoft Office, Word; ASSECO Poland S. A.- Płatnik	Z CUW-Żabia Wola do ZUS za pośrednictwem programu Płatnik przez Internet, komunikacja automatyczna, dwukierunkowa
2.	Umowy z wykonawcami, bankami	Pomieszczenie nr 3	imię/nazwisko/adres/	Microsoft, Office	Z CUW-Żabia Wola do wykonawców za pośrednictwem platformy internetowej poczty elektronicznej……@....., komunikacja manualna, dwukierunkowa
3.	Ewidencja korespondencji przychodzącej i wychodzącej	Pomieszczenie nr 1, 2, 3	imię/nazwisko/adres		
4.	Pocztowa książka nadawcza	Pomieszczenie nr 1,2,3	imię/nazwisko/adres	Elektroniczny Nadawca Poczta Polska	Z CUW - Żabia Wola do Urzędu Pocztowego w Żabiej Woli przez

					Internet, komunikacja manualna, jednokierunkowa
5.	Ewidencja uczestników zamówień publicznych	Pomieszczenie nr 1,3	imię/nazwisko/numer telefonu/ Adres/NIP/adres poczty elektronicznej,	Microsoft, Office; http://www.zabiawola.pl/358,centrum-uslug-wspolnych-w-gminie-zabia-wola	Z CUW- Żabia Wola do Ministerstwa Cyfryzacji w ramach publikowania informacji w BIP przez Internet, komunikacja jednokierunkowa
6.	Zarządzenia Kierownika CUW	Pomieszczenie nr 1	imię/nazwisko	Microsoft, Office; http://www.zabiawola.pl/358,centrum-uslug-wspolnych-w-gminie-zabia-wola	Z CUW- Żabia Wola do Ministerstwa Cyfryzacji w ramach publikowania informacji w BIP przez Internet, komunikacja jednokierunkowa
7.	Dokumentacja certyfikatów kwalifikowanych (*e-podpisy*)	Pomieszczenie nr 1	imię/nazwisko/PESEL/login/email/nr telefonu		
8.	Rejestr upoważnień, pełnomocnictw	Pomieszczenie nr 1	imię/nazwisko/stanowisko/zakres upoważnienia	Microsoft, Office	
9.	Rejestr delegacji służbowych	Pomieszczenie nr 3	imię/nazwisko/stanowisko/nazwa pracodawcy		
10.	Rejestr pieczątek	Pomieszczenie nr 1	imię/nazwisko/stanowisko/nazwa pracodawcy		
11 12	Ewidencja pracowników upoważnionych do przetwarzania danych osobowych	Pomieszczenie nr 1	imię/nazwisko	Microsoft, Office	

13	Dokumentacja służąca sporządzaniu listy płac	Pomieszczenie nr 1,3	imię/nazwisko/stanowisko/wymiar zatrudnienia/nazwa pracodawcy	Microsoft, Office; Vulcan Sp. z o.o. – program Płace Optivum	
14	Listy płac pracowników	Pomieszczenie nr 1,2,3	imię/nazwisko/PESEL/stanowisko	Vulcan Sp. z o.o. – program Płace Optivum	
15	Informacja o dochodach oraz pobranych zaliczkach na podatek dochodowy (*PIT-11*)	Pomieszczenie nr 3	imię/nazwisko/ PESEL/NIP/nazwisko rodowe/data i miejsce urodzenia/adres/wysokość zarobków		Z CUW – Żabia Wola do Urzędu Skarbowego za pośrednictwem Płace Optivum (przesyłka elektroniczna) przez interent, komunikacja dwukierunkowa
16	Dokumentacja na potrzeby Zakładu Ubezpieczeń Społecznych	Pomieszczenie nr 3	imię/nazwisko/ PESEL/data i miejsce urodzenia/adres zamieszkania/wysokość zarobków/nazwa pracodawcy	Microsoft, Office	
17	Deklaracje i kartoteki ZUS pracowników	Pomieszczenie nr 3	imię/nazwisko/nazwisko rodowe/imiona rodziców/data urodzenia/miejsce urodzenia/PESEL/NIP/adres Zameldowania/adres zamieszkania/obywatelstwo/imiona i nazwiska/data urodzenia dzieci pracownika/wymiar czasu pracy	ASSECO Poland S. A.- Płatnik	Z CUW – Żabia Wola do ZUS za pośrednictwem programu Płatnik przez interent, komunikacja dwukierunkowa
18	Kartoteki zarobkowe pracowników	Pomieszczenie nr 3	imię/nazwisko/data urodzenia/PESEL/miejsce zamieszkania/stopień awansu/składniki wynagrodzeń i potrąceń/okres zwolnienia/imię i		

			nazwisko/specjalność i nr lekarza wystawiającego zwolnienie lekarskie		
19	Umowy cywilnoprawne	Pomieszczenie nr 1,2,3	imię/nazwisko/data i miejsce urodzenia/miejsce zamieszkania (adres do korespondencji)/numer pesel/nip/dane dot. konta bankowego/wysokość i składniki wynagrodzenia/seria i numer dowodu osobistego	Microsoft, Office	
20	Dokumentacja księgowa (przelewy, faktury, KP, KW)	Pomieszczenie nr 1,2,3	imię/nazwisko/adres/nazwa/nr konta bankowego kontrahentów/ NIP/REGON/nr telefonu	Księgowość firmy U.I. INFO-SYSTEM Roman i Tadeusz Groszek sp.j.; System bankowości elektronicznej Banku Spółdzielczego w Białej rawskiej http://www.bs-bialarawska.com.pl	Z CUW-Żabia Wola do Banku Spółdzielczego w Białej Rawskiej Filia w Żabiej Woli za pośrednictwem bankowości internetowej http://www.bs-bialarawska.com.pl – komunikacja dwukierunkowa.
21	Dane kontrahentów CUW oraz podmiotów współpracujących	Pomieszczenie nr 1,2,3	Nazwisko/imię/adres/nazwa/nr konta bankowego kontrahentów/ NIP/REGON/nr telefonu	Księgowość firmy U.I. INFO-SYSTEM Roman i Tadeusz Groszek sp.j.	
22	Akta osobowe pracowników	Pomieszczenie nr 1,3	PESEL/imię i nazwisko/nazwisko rodowe/ data i miejsce urodzenia/płeć/adres stały/ numer telefonu/ e-mail/ dowód osobisty (seria i nr, wydany przez, data	Microsoft, Office	

			wydania)/ imię ojca/ imię matki/ stan cywilny i rodzinny/stosunek do służby wojskowej (dokument wojskowy, seria i numer, stopień wojskowy)/ numer legitymacji służbowej/ posiada gospodarstwo rolne/ emeryt/ rencista/ obywatelstwo obce/ osoba kontaktowa/ wykształcenie/ nazwa szkoły i rok ukończenia/ warunki zatrudnienia/ staż pracy/ historia pracy, kary, nagrody/ tytuł zawodowy/ zawód wyuczony i wykonywany/ uzyskane kwalifikacje/ nieobecności w pracy		
23	Podania osób ubiegających się o pracę	Pomieszczenie nr 1	data i miejsce urodzenia / adres zamieszkania / wykształcenie/ telefon / e-mail / przebieg kariery zawodowej/ dodatkowe kwalifikacje		
24	Ewidencja czasu pracy pracowników CUW	Pomieszczenie nr 3	Imię i nazwisko		
25	Ewidencja urlopów	Pomieszczenie nr 3	Imię i nazwisko/stanowisko/wymiar urlopu/wykorzystanie urlopów		
26	Dokumentacja Zakładowego Funduszu Świadczeń Socjalnych	Pomieszczenie nr 1,3	PESEL / NIP / imię i nazwisko / data i miejsce urodzenia / adres zamieszkania /		

			informacje o stanie zdrowia / informacje o wysokości dochodów		
27	Zbiór danych związany z realizacją projektów unijnych	Pomieszczenie nr 1,2,3	Nazwisko/imiona/płeć/wiek/PESEL / wykształcenie/adres zameldowania/adres zamieszkania/numery telefonów/adres e-mail	Microsoft, Office	
28	Obowiązek nauki	Pomieszczenie nr 1	Nazwisko/imiona/data urodzenia/PESEL/ Adres zameldowania/imiona rodziców	Microsoft, Office	
29	Wypadki uczniów	Pomieszczenie nr 1	Nazwisko/imiona/data urodzenia		
30	Fundusz zdrowotny nauczycieli	Pomieszczenie nr 1	Nazwisko/imiona/ data urodzenia/adres zamieszkania/ nr telefonu/ informacje o stanie zdrowia	Microsoft, Office	
31	Dokumentacja postępowania na stopień nauczyciela mianowanego	Pomieszczenie nr 1	Nazwisko/imiona/ data urodzenia/adres zamieszkania/ wykształcenie	Microsoft, Office	

ZAŁĄCZNIK NR 5
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

. . . . , dnia . . . .

. . . .
(pieczątka)

UPOWAŻNIENIE NR . . . . . .

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. 2016, poz. 922) upoważniam:

Pana / Panią . . . .

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku: ……………………………………..w następującym zakresie:

Nazwa zbioru:	Identyfikator*:	Zakres upoważnienia
		zbieranie/ utrwalanie/ przechowywanie/ opracowywanie/ zmienianie/ udostępnianie/ usuwanie/ wgląd

Upoważnienie udzielane jest na czas pełnienia obowiązków służbowych od dnia . . . . .r.

* uzupełnić w przypadku gdy zbiór przetwarzany jest w systemie informatycznym.

. . . .

(data i podpis
Administratora Danych Osobowych)

(data i podpis osoby upoważnionej)

ZAŁĄCZNIK NR 6
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych
w Gminie Żabia Wola

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

L.p.	Nazwisko i imię / identyfikator	Numer upoważnienia	Data nadania (modyfikacji) upoważnienia	Data utraty ważności upoważnienia	Zbiór danych osobowych oraz zakres upoważnienia do przetwarzania danych osobowych
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

ZAŁĄCZNIK NR 7
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

LISTA UCZESTNIKÓW SZKOLENIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Miejsce i data szkolenia: ……

Prowadzący: ……

L.p.	Imię i nazwisko uczestnika:	Podpis:

ZAŁĄCZNIK NR 8
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

. . . . . .
(Imię i nazwisko pracownika)

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH

Oświadczam, iż w związku z wykonywanymi obowiązkami służbowymi, przetwarzam lub mam dostęp do zbiorów, dokumentów, zestawień, kartotek lub systemów informatycznych zawierających dane osobowe i w związku z tym zapoznałem(am) się z:

1) przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z ustawą z 29 sierpnia 1997r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2016 r. poz. 922);
2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do ich przestrzegania (Dz. U. 2004 r. Nr 100, poz. 1024);
3) dokumentem „Polityką Bezpieczeństwa i Ochrony Przetwarzania Danych Osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola„ wprowadzoną Zarządzeniem Nr…. Dyrektora Centrum Usług Wspólnych w Gminie Żabia Wola z dnia . . .
4) dokumentem „Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola”.

Zobowiązuje się do nieujawniania informacji, z którymi zapoznałem/am się przy okazji wykonywanej pracy. W szczególności zobowiązuję się nie ujawniać:

1) danych osobowych zawartych w systemach informatycznych,
2) szczegółów technologicznych używanych w systemach informatycznych eksploatowanych jednostce,
3) używanego oprogramowania przeznaczonego do przetwarzania danych osobowych w jednostce,
4) haseł i loginów do systemów w których przetwarzane są dane osobowe.

Jednocześnie zobowiązuję się do stosowania określonych przez Administratora Danych Osobowych zasad, procedur oraz wytycznych mających na celu:

1) właściwe i adekwatne w stosunku do celu przetwarzanie danych;
2) należyte zabezpieczanie danych osobowych przed ich udostępnianiem osobom nieupoważnionym;

3) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych w celu ochrony osób, których dane dotyczą;
4) zachowania w tajemnicy danych oraz ich sposobu zabezpieczeń, nawet po ustaniu stosunku pracy.

Oświadczam również, iż znany jest mi telefoniczny numer kontaktowy do Administratora Danych Osobowych.

. . . . . .

(data i podpis)

ZAŁĄCZNIK NR 9
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

EWIDENCJA OSÓB ZAPOZNANYCH Z PRZEPISAMI DOTYCZĄCYMI OCHRONY DANYCH OSOBOWYCH ORAZ POLITYKĄ BEZPIECZEŃSTWA

Lp.	Nazwisko i imię	Data i podpis

ZAŁĄCZNIK NR 10
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych w Gminie Żabia Wola

EWIDENCJI POBRANIA/ ZDANIA SPRZĘTU, DOKUMENTÓW

Lp.	Data pobrania	Imię i nazwisko pracownika	Stanowisko	Data zdania

ZAŁĄCZNIK NR 11
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

SPEŁNIENIE OBOWIĄZKU INFORMACYJNEGO (PRZY ZBIERANIU DANYCH OD OSÓB, KTÓRYCH ONE DOTYCZĄ)

Zgodnie z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) informuję, iż:
Administratorem Pani/Pana danych osobowych jest Centrum Usług Wspólnych w Gminie Żabia Wola z siedzibą przy ul. Mazowieckiej 1, 96- 321 Żabia Wola.

Pani/Pana dane osobowe przetwarzane będą w celu …….. i nie będą udostępniane podmiotom innym niż uprawnione na mocy przepisów prawa.

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania

Podanie danych osobowych jest dobrowolne/ obowiązkowe* zgodnie z…….
(podstawa prawna)

…….

(podpis osoby informowanej)

*) niepotrzebne skreślić

ZAŁĄCZNIK NR 12
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

WNIOSEK
O UDOSTĘPNIENIE DANYCH ZE ZBIORU DANYCH OSOBOWYCH

1. Wniosek do: . . . . . .

2. Wnioskodawca . . . . . .

. . . . . .
(nazwa firmy i jej siedziba albo nazwisko, imię i adres zamieszkania wnioskodawcy ew. NIP oraz REGON)

3. Podstawa prawna upoważniająca do pozyskania danych:

. . . . . .
. . . . . .

4. Wskazanie przeznaczenia dla udostępnionych danych osobowych:

. . . . . .
. . . . . .

5. Oznaczenia lub nazwa zbioru, z którego mają być udostępnione dane osobowe:

. . . . . .
. . . . . .

6. Zakres żądanych informacji ze zbioru:

. . . . . .
. . . . . .

7. Informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych:

. . . . . .
. . . . . .

. . . . . .
(data i podpis wnioskodawcy)

ZAŁĄCZNIK NR 13
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola

EWIDENCJA UDOSTĘPNIENIA DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA

L.p.	Data wydania	Dane odbiorcy	Zakres udostępnionych danych	Podpis osoby udostępniającej dane osobowe

ZAŁĄCZNIK NR 14
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

. . . . . , dn. . . . . .r.

. . . . . .
(pieczątka)

. . . . . .
(imię i nazwisko)
. . . . . .
. . . . . .
. . . . . .
(adres)

INFORMACJA
O ZAWARTOŚCI ZBIORU DANYCH OSOBOWYCH

Działając na podstawie art. 33 ust. 1 Ustawy o ochronie danych osobowych oraz w związku z Pani/ Pana wnioskiem z dnia…… o udzielenie informacji związanych z przetwarzaniem Pani/ Pana danych osobowych w Centrum Usług Wspólnych w Gminie Żabia Wola informuję, że zbiór danych zawiera następujące Pani/Pana dane osobowe: . . . . . .
. . . . . .
. . . . . .
Powyższe dane przetwarzane są od……w . . . . . w
celu . . . . . z zachowaniem
wymaganych zabezpieczeń i zostały uzyskane ……....
……
Powyższe dane nie były/były udostępniane* . . . . . .
w celu . . . . . …

Zgodnie z art. 32 ust. 1 Ustawy o ochronie danych osobowych przysługuje Pani/Panu prawo do kontroli danych osobowych, prawo ich poprawiania, a także w przypadkach kreślonych w art. 32 ust. 1 pkt 7 i 8 Ustawy, prawo wniesienia umotywowanego żądania zaprzestania przetwarzania danych oraz prawo sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych innemu administratorowi danych osobowych.

*) niepotrzebne skreślić

. . . . . .

(podpis Administratora Danych
Osobowych lub upoważnionej przez
niego osoby)

ZAŁĄCZNIK NR 15
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w ……....(miejscowość), w dniu ……...r. pomiędzy **……..…… (nazwa jednostki organizacyjnej)** reprezentowanym przez ……..(imię i nazwisko) zwanym w dalszej części **Zleceniodawcą,**
a
……..... (nazwa podmiotu) reprezentowanym przez ……. (imię i nazwisko), zwanym w dalszej części **Wykonawcą**.

§ 1.

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy (.....) a (.....), o ..... Zleceniodawca powierza Wykonawcy w trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (t. j. Dz. U. z 2016 r. poz. 922) zwanej dalej „ustawą" przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o ……...
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2.

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych/:
   1) imię i nazwisko,
   2) numer ewidencyjny PESEL,
   3) seria i numer dowodu osobistego,
   4) ..... .

2. Zakres przetwarzania powierzonych danych obejmuje: np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie, wgląd (wybrać czynności).
3. **Wykonawca** może przetwarzać dane osobowe przekazane przez powierzającego wyłącznie w celu …….. określonym w ……..

§ 3.

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się do:
   1) przetwarzania powierzonych mu danych osobowych zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

2) zabezpieczenia danych osobowych poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36 – 39 a ustawy o ochronie danych osobowych.
3) dopuszczania do przetwarzania danych wyłącznie osób posiadających imienne upoważnienie do przetwarzania powierzonych danych;
4) zapewnienia kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
5) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych;
6) niezwłocznego informowania Zleceniodawcy o wszystkich okolicznościach mających wpływ na bezpieczeństwo przetwarzanych danych, jak również o ewentualnej kontroli przeprowadzonej przez Generalnego Inspektora Danych Osobowych u Wykonawcy.

2. Zleceniodawca upoważnia wykonawcę do wydawania osobom, biorącym udział w przetwarzaniu danych, upoważnień do przetwarzania powierzonych danych osobowych. Wykonawca ograniczy dostęp do danych osobowych wyłącznie do osób posiadających imienne upoważnienia do przetwarzania danych osobowych
3. Wykonawca zobowiązany jest do niezwłocznego przekazania Zleceniodawcy kopii potwierdzonych za zgodność z oryginałem wystawionych upoważnień, o których mowa w ust. 2 niniejszego paragrafu.
4. Wykonawca oświadcza, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024):
   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony, jako wysoki,
   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
5. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
   1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,
   2) każdym nieupoważnionym dostępie do danych osobowych,
   3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.

6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

§4.

Odpowiedzialność

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. Odpowiedzialność prawną z tytułu realizacji obowiązków wynikających z niniejszej umowy oraz z ustawy o ochronie osobowych ponoszą jednocześnie Administrator i Procesor.
3. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§5.

Czas obowiązywania Umowy powierzenia

Niniejsza Umowa powierzenia zostaje zawarta na okres obowiązywania Uchwały nr ….. Rady Gminy ….. z dnia ….. / do dnia …. / na okres obowiązywania umowy nr …. z dnia …

§ 6.

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej umowy jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1 niniejszej umowy.

§ 7.

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa w § 1 ust. 1 lub niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie

usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8.

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9.

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego oraz ustawy z dnia 29 stycznia 2004 roku ustawy o ochronie danych osobowych.

§10.

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11.

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....	.....
podpis Zleceniodawcy	podpis Wykonawcy

ZAŁĄCZNIK NR 16
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych
w Gminie Żabia Wola

PLAN SPRAWDZEŃ W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA
NA OKRES DD. MM. – DD. MM. RR

Lp.	Termin (rozpoczęcia-zakończenia)	Przedmiot sprawdzenia:	Zakres sprawdzenia:	Sposób dokumentowania: Zakres dokumentowania:	Wydział/ stanowisko /pomieszczenie podlegające sprawdzeniu
1.	dd. mm- dd. mm. rr	Zbiór danych osobowych: np. akta osobowe pracowników	Legalność przetwarzania danych- art. 23 i 27 UODO		
2.	dd. mm- dd. mm. rr	Zbiór danych osobowych: np. akta osobowe pracowników	Realizacja praw osób, których dane przetwarzamy – Rozdział 4 UODO		
3.	dd. mm- dd. mm. rr	Techniczne i organizacyjne zabezpieczenie pomieszczeń i stanowisk pracy, w których przetwarzane są dane osobowe	Spełnieni wymogów zgodnie z Rozporządzeniem (……..)	1.Przeprowadzenie wizji lokalnej w pomieszczeniach biurowych, w których przetwarzane są dane osobowe. 2. Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń. nośników oraz systemów informatycznych służących do przetwarzania danych osobowych.	

				3. Sporządzenie sprawozdania	
4.	dd. mm- dd. mm. rr	Funkcjonowanie zastosowanych zabezpieczeń technicznych służących do ochrony systemów informatycznych służących do przetwarzania lub zabezpieczenia danych (systemy informatyczne)	Ocena systemu informatycznego służącego do przetwarzania i ochrony danych osobowych: 1. zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, 2. zabezpieczenie danych przed ich przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, 3. przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie, 4. odnotowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywanych na danych osobowych przez użytkowników, 5. kontrola jakie dane osobowe, kiedy i przez kogo zostały do zbioru w systemie wprowadzone oraz komu są przekazywane 6. spełnienie wymogów ochrony danych systemów informatycznych służących do przetwarzania danych osobowych, 7. sprawdzenie mechanizmów automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika,	1. Sporządzenie notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych. 2. Odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem. 3. Sporządzeniu kopii otrzymanego dokumentu; sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych. 4. Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu. 5. Sporządzenie sprawozdania.	

			8. tworzenie kopii zapasowych, 9. zabezpieczenie systemowe i fizyczne sprzętu komputerowego.		
5.	dd. mm- dd. mm. rr	System Informatyczny: (nazwa)	Wymogi stawiane systemom informatycznym		

Dokumentowanie czynności w toku sprawdzenia zawiera w szczególności:

Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

Odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;

Sporządzeniu kopii otrzymanego dokumentu, sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;

Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

……..……..

(Administrator Danych Osobowych)

ZAŁĄCZNIK NR 17
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

ZGŁOSZENIE
NARUSZENIA/ PODEJRZENIA NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W CENTRUM USŁUG WSPÓLNYCH W GMINIE ŻABIA WOLA

1. Data: . . . . Godzina: . . . .
(dd.mm.rr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

. . . .
(imię i nazwisko, stanowisko służbowe)

3. Lokalizacja zdarzenia :

. . . .

4. Opis zaistniałej sytuacji wpływającej na bezpieczeństwo danych osobowych:

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .

. . . .
godz. i data przyjęcia zgłoszenia Podpis osoby zgłaszającej

…………………………
podpis Administratora Danych Osobowych

ZAŁĄCZNIK NR 18
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych
w Centrum Usług Wspólnych
w Gminie Żabia Wola

. . . . . , dn. . . . . .r.

SPRAWOZDANIE ZE SPRAWDZANIA ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

1. Oznaczenie administratora danych i adres jego siedziby:
……..……
……..
(pełna nazwa oraz adres)

2. Rodzaj sprawdzenia:
planowe/ doraźne*

CZĘŚĆ 1: SPRAWDZENIE PLANOWE

1. Datę rozpoczęcia sprawdzenia: ……..
2. Określenie przedmiotu i zakresu sprawdzenia:
……..……
……....
3. Wykaz czynności podjętych przez Administratora Danych Osobowych w toku sprawdzenia:……
……
……
……
……
……
4. Opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:……
…..……
……
……
……

5. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:…….
   ……
   ……
   ……
   ……
   ……

8. Wyszczególnienie załączników stanowiących składową część sprawozdania:
   ……
   ……
   ……
9. Imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:
   ……
   ……
   ……
   ……
   ……
   …….
10. Data zakończenia sprawdzenia: …….

…… ……
(miejscowość, data) (podpis Administratora Danych Osobowych)

CZĘŚĆ 2: SPRAWDZENIE DORAŹNE

1. Data i godzina powiadomienia o naruszeniu lub podejrzeniu naruszenia ochrony przetwarzania danych osobowych: ……..
2. Godzina przybycia ADO na miejsce zdarzenia: …….
3. Opis sytuacji zastanej:
   ……
   ……
   ……
   ……
   …….
4. Przyczyny i skutki zdarzenia:
   ……
   ……
   ……
   ……

……
……
…….

5. Wnioski i propozycje działań naprawczych (zapobiegawczych)/ propozycje rozwiązań dotyczących lepszego zabezpieczenia danego obszaru:
   ……
   ……
   ……
   ……
   …….
6. Wyszczególnienie załączników stanowiących składową część sprawozdania:
   ……
   ……
   ……

7. Imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach:
   ……
   ……
   ……
   ……
   ……
   …….
8. Godzina zakończenia sprawdzenia: …….

…… ……

(miejscowość, data) (podpis Administratora Danych Osobowych)

*) niepotrzebne skreślić i wypełnić odpowiednio CZĘŚĆ 1 lub CZĘŚĆ 2 niniejszego sprawozdania.

ZAŁĄCZNIK NR 19
do Polityki Bezpieczeństwa i Ochrony
Przetwarzania Danych Osobowych w Centrum Usług Wspólnych
w Gminie Żabia Wola

REJESTR SPRAWDZEŃ

L.p.	Nazwa sprawdzanego działu	Nazwisko, imię i stanowisko osoby przeprowadzającej sprawdzenie	Czas trwania sprawdzenia	Uwagi	Podpis osoby przeprowadzającej sprawdzenie